The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
05/26/2016

SUBJECT:
Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could result in arbitrary code execution. Google Chrome is a web browser used to access the Internet. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the browser, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:

- Google Chrome prior to version 51.0.2704.63

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Google Chrome. These vulnerabilities can be triggered by a user visiting a specially crafted web page. Details of these vulnerabilities are as follows:

- Cross-origin bypass in extension bindings. (CVE-2016-1672)(CVE-2016-1676)
- Cross-origin bypass in Blink. (CVE-2016-1673) (CVE-2016-175)
- Cross-origin bypass in extensions. (CVE-2016-1674)
- Type confusion in V8. (CVE-2016-1677)
- Heap overflow in V8. (CVE-2016-1678)
- Heap use-after-free in V8 bindings. (CVE-2016-1679)

- Heap use-after-free in Skia. (CVE-2016-1680)
- Heap overflow in PDFium. (CVE-2016-1681)
- CSP bypass for ServiceWorker. (CVE-2016-1682)
- Out-of-bounds access in libxslt. (CVE-2016-1683)
- Integer overflow in libxslt.(CVE-2016-1684)
- Out-of-bounds read in PDFium. (CVE-2016-1685) (CVE-2016-1686)
- Information leak in extensions. (CVE-2016-1687)
- Out-of-bounds read in V8. (CVE-2016-1688)
- Heap buffer overflow in media (CVE-2016-1689)
- Heap use-after-free in Autofill. (CVE-2016-1690)
- Heap buffer-overflow in Skia. (CVE-2016-1691)
- Limited cross-origin bypass in ServiceWorker. (CVE-2016-1692)
- HTTP Download of Software Removal Tool. (CVE-2016-1693)
- HPKP pins removed on cache clearance. (CVE-2016-1694)
- Various fixes from internal audits, fuzzing and other initiatives. (CVE-2016-1695)

Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the browser, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Google to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

Google:
http://googlechromereleases.blogspot.in/2016/05/stable-channel-update_25.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1672
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1673
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1674
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1675
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1676
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1677
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1678
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1679
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1680
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1681

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1682
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1683
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1684
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1685
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1686
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1687
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1688
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1689
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1690
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1691
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1692
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1693
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1694
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1695